UNIVERSITY OF WOLLONGONG AUSTRALIA

PRIVACY MANAGEMENT PLAN

Date first approved: 7 December 2012	**Date of effect:** 7 December 2012	**Date last amended:** (refer Version Control Table)	**Date of Next Review:** December 2019
First Approved by:	University Council		
Custodian title & e-mail address:	Director, Governance and Legal Division privacy-enquiry@uow.edu.au		
Author:	Director, Governance and Legal Division		
Responsible Division & Unit:	Legal Services Unit, Governance and Legal Division		
Supporting documents, procedures & forms of this procedure:	Privacy Policy University Code of Conduct Privacy Complaint Internal Review Application Form		
Relevant Legislation & **External Documents:**	Privacy and Personal Information Protection Act 1998 (NSW) ("PPIPA") Health Records and Information Privacy Act 2002 (NSW) ("HRIPA") Information and Privacy Commission NSW Government Information (Public Access) Act 2009 (NSW) Independent Commission Against Corruption Act 1988 (NSW) Public Interest Disclosures Act 1994 (NSW) State Records Act 1998 (NSW) Workplace Surveillance Act 2005 (NSW) Work Health and Safety Act 2011 (NSW) University of Wollongong Act 1989 (NSW) University of Wollongong By Law 2005 (NSW) Rules of the University of Wollongong University Code of Conduct Records Management Policy Fraud and Corruption Prevention Policy Workplace Health and Safety Policy		
Audience:	Public		

UNIVERSITY OF WOLLONGONG AUSTRALIA

Contents

UNIVERSITY OF WOLLONGONG AUSTRALIA

1 Introduction / Background

1. The University of Wollongong ("UOW"), as part of its functions, manages *personal* and/or *health information* received from *staff*, students and third parties, and must comply with the *Privacy and Personal Information Protection Act* 1998 ("PPIPA"), the *Health Records and Information Privacy Act* 2002 ("HRIPA") and other relevant laws, including but not limited to regulations, statutory guidelines, codes of practice and privacy directions.
2. UOW has produced this Privacy Management Plan to comply with section 33 of PPIPA. The purpose of this Plan is to outline:
   a. how UOW complies with PPIPA and HRIPA in its activities;
   b. how UOW disseminates its policies and practices regarding privacy within UOW; and
   c. what procedures UOW follows for internal reviews or complaints about UOW 's privacy practices.
3. UOW will provide a copy of this Privacy Management Plan to the Privacy Commissioner as soon as practicable after it is prepared and whenever the plan is amended, in compliance with section 33(5) of PPIPA.
4. This Privacy Management Plan operates as a procedure document supporting UOW 's Privacy Policy and is to be read in conjunction with UOW's Privacy Policy.
5. The Privacy Policy and this Privacy Management Plan can be found on UOW's Policy Directory and Privacy Homepage located on the UOW website. Any requests for hard copies of these documents can be forwarded to privacy-enquiry@uow.edu.au.

2 Compliance with this Privacy Management Plan

1. All *staff* of UOW must comply with this Privacy Management Plan.
2. The Principal Privacy Officer (or delegate) may audit UOW 's compliance with this Privacy Management Plan.
3. A breach of the Privacy Policy or this Privacy Management Plan may constitute misconduct pursuant to UOW codes, policies and guidelines and be subject to disciplinary action.
4. This Plan does not apply to UOW's *related entities*. UOW's *related entities* have their own policies and procedures regarding *information* that is provided to or collected by them.

3 Definitions

Word/Term	Definition (with examples if required)
Information	*Health information* and/or *personal information* as the context permits.
Investigative Agency	Investigative agencies include (but are not limited to) the Ombudsman 's Office, the Independent Commission Against Corruption, the Police Integrity Commission, the Health Care Complaints Commission, the Australian Health Practitioners Regulation Agency, the Anti-Discrimination Board and the Community Services Commission.

Law enforcement agency	Law enforcement agencies include the Police Force of NSW or of another State or Territory, the NSW Crime Commission, the Australian Federal Police, the Australian Crime Commission, the Director of Public Prosecutions of NSW, another State or Territory or the Commonwealth, the Department of Justice and/or the Office of the Sheriff of NSW.
Personal information	Personal information, for the purpose of this policy, refers to personal information defined in PPIPA (or as amended in PPIPA from time to time) as: "Information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion." Under PPIPA, personal information does not include: i. information regarding an individual who has been deceased for more than 30 years; ii. information about an individual that is readily available in a publicly available publication; and iii. information or an opinion about an individual's suitability for appointment or employment as a public sector official.
Related entities	UOW's related entities include UOW Enterprises, UOW Pulse and the Illawarra Health and Medical Research Institute (IHMRI).
Sensitive information	A subclass of *personal information* relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities.
Staff	All employees of UOW (including casual and conjoint employees) and honorary and visiting appointees, consultants and contractors, agency staff, emeriti, members of UOW committees and any other person appointed or engaged by UOW to perform duties or functions for UOW.

4 The Information Protection Principles and Health Privacy Principles

1. Under PPIPA, there are twelve Information Protection Principles (IPPs) that apply to public sector agencies such as UOW. The Information Protection Principles are contained in sections 8-19 of PPIPA.
2. Under HRIPA, there are fifteen Health Privacy Principles (HPPs) that apply to agencies that are either a health service provider or that collect, hold or use health information, such as UOW. The Health Privacy Principles are contained in Schedule 1 of HRIPA.
3. The application of the IPPs and HPPs at UOW are discussed in the next sections of this Plan. As the first twelve IPPs are substantially similar to the first twelve HPPs, those principles, where relevant, are discussed together and numbered together.

5 Collection of *Information* for Lawful Purposes

1. IPP 1 and HPP 1 state that UOW must not collect *information* unless:
   a. the *information* is collected for a lawful purpose that is directly related to a UOW function or activity; and
   b. the collection of the *information* is reasonably necessary for that purpose.
2. If *information* received by UOW is unsolicited, the principles relating to collection do not apply. However, if UOW decides to make use of, or take any action in relation to the unsolicited *information,* then UOW is regarded to have 'collected' the *information* and the collection principles will then apply.If UOW decides to keep any unsolicited *information* he provisions of PPIPA and HRIPA relating to the storage, use and disclosure of that *information* will apply

Application by UOW

3. Lawful purpose directly related to a UOW function or activity:

The objects and functions of UOW are set out in the *University of Wollongong Act 1989*. Examples of the purposes for which *information* is collected and used by UOW include:

a. education delivery;
b. conferring of degrees and other awards;
c. research;
d. promotion and commercialisation of UOW property;
e. fundraising;
f. promotion of UOW events and programs (and associated compilation of UOW reunion and alumni invitation lists);
g. surveys and competitions;
h. news and updates;
i. selection, employment, appraisal and remuneration of staff;
j. student accommodation;
k. support services such as counselling/disability services;
l. scholarship applications;
m. managing complaints or disputes; and
n. requests for academic consideration.

2. UOW welcomes enquiries and feedback (which includes comments, compliments and complaints) from *staff*, students and third parties. *Information* is collected and used to respond to any matters raised through these communication systems, to improve UOW services and promote effective complaint handling processes.

UNIVERSITY OF WOLLONGONG AUSTRALIA

6 Collection of *Information* Directly from Individual

1. IPP 2 and HPP 3 state that UOW must, when collecting *information*, collect the *information* directly from the individual to whom the *information* relates, unless:
    a. the individual authorised collection of the personal information from someone else; or
    b. the personal information is provided by a parent or guardian of a person who is under the age of 16 years; or
    c. it is unreasonable or impracticable to collect health information directly. An example of this may include where an individual lacks the capacity to provide his/her health information due to health reasons, in which case that health information may be collected form an authorised representative such as a carer or guardian.

Exceptions

2. Exceptions to IPPS 2 and HPP 3 include where:
    a. the information is collected in connection with actual or anticipated proceedings before any court or tribunal;
    b. UOW is investigating a complaint which has or may be referred or made to or from an investigative agency;
    c. compliance by UOW would prejudice the interests of the individual to whom the information relates;
    d. non-compliance is otherwise permitted (or necessarily implied or reasonably contemplated) under an Act or any other law; or
    e. indirect collection is otherwise lawfully authorised or required.

Application by UOW

3. UOW collects *information* directly from:
    a. prospective employees and staff;
    b. prospective students, enrolling or enrolled students;
    c. alumni; and/or
    d. members of the public interacting with UOW. An example of this may include a client of UOW's Northfields Clinic.
4. UOW facilitates the collection of *information* directly from the individual through the provision of:
    a. forms;
    b. user-based electronic mail services for all staff and students through a secure server;
    c. secure web-based data collection systems via UOW's website; and/or
    d. telephone and face-to-face interaction.
5. At times, UOW collects *information* indirectly, but only does so when UOW is lawfully

authorised or required to do so. That authorisation may come from:

a. the consent that students provide as part of the application and/or enrolment process;

b. the consent provided from an applicant by prospective employees; and

c. within PPIPA and HRIPA.

6. Under these authorisations, *information* can be indirectly collected from:

a. other tertiary institutions, UOW agents and *related entities*;

b. some relevant government departments such as the Commonwealth government department with responsibility for immigration;

c. family members acting with the authority of the individual; or

d. *law enforcement agencies or investigative agencies.*

7 Requirements When Collecting *Information*

1. IPP 3 and HPP 4 state that if UOW collects information from an individual, UOW must take all steps as are reasonable in the circumstances to ensure that, before the *information* is collected or as soon as practicable after collection, the individual to whom the *information* relates is made aware of the following ("Collection Statement"):

a. the fact that *information* is being collected;

b. the purposes for which the *information* is being collected;

c. all intended recipients of the *information*;

d. whether the supply of the *information* by the individual is required by law or is voluntary;

e. consequences for the individual if the *information* (or any part of it) is not provided;

f. the existence of any right of access to, or correction of, the *information*; and

g. the name and address of the agency that is collecting the *information* and the agency that is to hold the *information*.

2. In practical terms, this means that UOW should provide a Collection Statement at each point where *information* is collected from an individual, unless an exception applies.

Exceptions

2. Exceptions to IPP 3 and HPP 4 include where:

a. the *information* is collected for law enforcement purposes;

b. the collection is reasonably necessary for the purpose of research, or the compilation or analysis of statistics, in the public interest and it is unreasonable or impracticable for the *information* to be collected directly from the individual to whom the *information* relates; or

c. UOW is investigating a complaint which has or may be referred to or from an *investigative agency*;

d. UOW is otherwise lawfully authorised or required not to notify the individual;

not notifying the individual is otherwise permitted (or necessarily implied or reasonably contemplated) under an Act or any other law;

a. compliance by UOW would prejudice the interest of the individual to whom the *information* relates;

b. the person has expressly consented to UOW not complying;

c. in the case of *health information*, (where the *health information* was collected from someone else) making the individual aware of the collection of that *health information* would pose a serious threat to the life or health of any individual;

d. in the case of *health information* (as per the guidelines issued under HRIPA) including circumstances:

   i. where *health information* is collected by a third party because it is unreasonable or impracticable to collect directly from the individual, then it would also be unreasonable or impracticable to notify the individual in the circumstances;

   ii. the *health information* was collected in the process of recording a family, social or medical history and this was necessary to provide health services to the individual;

   iii. where UOW reasonably believes that the individual is incapable of understanding the general nature of the matters included in a Collection Statement, provided UOW takes steps that are reasonable in the circumstances to ensure that any authorized representative of the individual is aware of those matters;

   iv. the *health information* was initially collected by another organization and there are reasonable grounds to believe that the individual has already been informed of the matters in a Collection Statement by the first collecting organization.

Application by UOW

2. UOW, including its faculties and business units, collect information at different times and in varying ways. As part of that *information* collection process, UOW will usually provide a Collection Statement to:

   a. Students at the point where *information* is collected, such as:

      i. a notice during the admission process, either online or in paper form;

      ii. an electronic notice provided as part of the enrolment or re-enrolment process;

      iii. a notice within a form, an agreement or as part of terms and conditions;

      iv. verbally where *information* is collected by phone; or

      v. by way of a sign where *information* is collected broadly and it is impractical to provide individual Collection Statements. Examples are areas under surveillance or being filmed for special occasions.

   b. Staff at the point where *information* is collected, such as:

      i. application for employment;

      ii. acceptance of offer of employment and terms of employment;

      iii. the administration of employment.

c. Others at the point where *information* is collected, such as members of the public:

i. participating in research conducted by, or being managed by, UOW;

ii. visiting the UOW website.

3. The following list provides examples of the common purposes for the collection of *information* by UOW:

a. the administration of a student's application, enrolment, academic progression and graduation;

b. providing support services to students and *staff*, such as disability services, academic consideration, counselling, Workplace Health and Safety and management of student placements;

c. the administration of employment such as payment of salary, superannuation, time recording, performance planning, performance management, leave application, recovery of debts and any other purposes necessary for UOW to function as an employer;

d. the activities of UOW and its *related entities* including administration, governance, provision of facilities, insurance, management of grievances or disciplinary procedures, financial systems, academic development, teaching and learning generally, sporting and cultural activities.

4. The UOW Privacy Homepage located at http://www.uow.edu.au/about/privacy/index.html provides links to the following Collection Statements:

a. Student Privacy and Disclosure Statement;

b. Privacy Collection Statement for Recruitment and Employee Records; and

c. UOW Website Privacy Collection Statement.

8 Other Requirements Relating to Collection of *Information*

1. IPP 4 and HPP 2 state that if UOW collects *information* from an individual, UOW must take such steps as are reasonable in the circumstances (having regard to the purposes for which the *information* is collected) to ensure that:

a. the *information* collected is relevant to that purpose, is not excessive, and is accurate, up-to-date and complete; and

b. the collection of the *information* does not intrude to an unreasonable extent on the personal affairs of the individual to whom the *information* relates.

Application by UOW

2. UOW will determine what steps are reasonable on a case-by-case basis. The factors which may be taken into account include:

a. the purpose for which the *information* was collected;

b. the sensitivity of the *information*;

c. how many people have access to the *information*;

d. the importance of accuracy to the proposed use;

e. the potential effects on the individual concerned if the*information* is inaccurate, out-of-date or irrelevant;

f. the opportunities to subsequently correct the *information*;

g. the ease with which the *information* can be checked.

3. UOW's Human Research Ethics Committee oversees and approves all research that is to be conducted by UOW where human participants are required. The Human Research Ethics Committee requires each researcher to outline the *information* to be collected by the researcher and assesses whether that collection is reasonable in the circumstances and whether the University's privacy obligations are addressed.

9 Retention and Security of *Information*

1. IPP 5 and HPP 5 state that if UOW holds *information* it must ensure that:

a. the *information* is kept for no longer than is necessary for the purposes for which the *information* may lawfully be used;

b. the *information* is disposed of securely and in accordance with any requirements for the retention and disposal of such *information*;

c. the *information* is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse; and

d. if it is necessary for the *information* to be given to a person in connection with the provision of a service to UOW (third party engagement), everything reasonably within the power of UOW is done to prevent unauthorised use or disclosure of the *information*.

Exceptions

2. Exceptions to HPP 5 apply in relation to *health information*, including where:

a. UOW is lawfully authorised or required not to comply; or

b. non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law.

Application by UOW

2. UOW is made up of a number of faculties and business units and each of these faculties and units may hold information in electronic format, hard copy or both, depending on that area 's practices and procedures and UOW's over-arching policies discussed below.

3. UOW is subject to the *State Records Act 1998*, which requires UOW to comply with timeframes for the retention and destruction of documents. UOW 's Records Management Policy is accessible online from the Policy Directory on UOWs website and provides further information regarding the University's obligations under the *State Records Act 1998*.

4. UOW is committed to ensuring all business activities performed with the use of information technology systems are protected and maintained, and that sustainable procedures are in place to reflect best practice information technology security. UOW 's information technology policies provide details of its commitment to the storage and protection of *information* in

compliance with its privacy obligations.

5. Staff are required to protect *information* by ensuring that:
   a. records are stored in University systems or University approved systems;
   b. access to systems or databases is restricted to those staff members with a legitimate business purpose;
   c. systems that are password protected are appropriately utilised and managed; and
   d. where appropriate, *information* is destroyed securely e.g. hard copy records are placed in security destruction bins.
6. Where UOW engages the services of a third party for the purpose of providing a particular service to UOW, all reasonable steps will be taken to ensure that the third party has robust practices in place to protect the information and prevent its unauthorised use or disclosure. The third parties to whom we disclose personal information may be located in Australia and other countries. Section 24 of this Privacy Management Plan provides further information on Third Party Engagement and Confidentiality.

10 Access to *Information* Held by UOW

1. IPP 6 and 7 and HPPs 6 and 7 state that if UOW holds *information*:
   a. it must take such steps as are, in the circumstances, reasonable to enable an individual to ascertain:
      i. whether UOW holds *information* relating to that individual;
      ii. if UOW holds *information* relating to that individual:
         - the nature of that *information*;
         - the main purpose for which the *information* is used; and
         - the individual's entitlement to gain access to the *information*;
   b. it must provide the individual with access to the *information* without excessive delay or excessive expense.

Exceptions

2. Exceptions to IPPs 6 and 7 and HPPs 6 and 7 include where:
   a. UOW is lawfully authorised or required not to comply; or
   b. non-compliance is otherwise permitted (or necessarily implied or reasonably contemplated) under an Act or any other law.

Application by UOW

2. These principles relate to access by an individual to his/her own records.
3. UOW will endeavour to respond to enquiries from an individual on whether it holds *information* about that individual, and the nature of any *information* held. Enquiries should be directed as follows:
   a. *Staff* who wish to obtain access to their personal *staff* records should contact UOW's

Human Resources Division at http://staff.uow.edu.au/personnel/contacts/index.html

b. Students who wish to obtain access to their personal records should contact Student Central on 1300 275 869 or email askuow@uow.edu.au.

c. Higher degree research (HDR) students who wish to obtain access to their personal records should contact the Graduate Research School at http://www.uow.edu.au/research/grs/index.html.

d. All other enquiries can be made to privacy-enquiry@uow.edu.au.

4. In most instances, UOW will provide access to an individual's *information* without a fee. However, there are some instances where UOW may charge a fee for the provision of certain *information* about an individual. An example is where UOW provides an individual with his/her official UOW academic transcript for a fee.

5. An individual also has a right to access *information* under the *Government Information (Public Access) Act 2009*. Lodgement and processing fees are chargeable using this method of access, which is detailed on UOW's dedicated Access to Information webpages and associated procedures.

6. Where someone contacts UOW and seeks access to *information* about another individual, this is a request for disclosure of *information*, and is managed under the disclosure principles discussed later in this Plan.

11 Alteration of *information* held by UOW

1. IPP 8 and HPP 8 state that:

a. where UOW holds *information*, it must, at the request of the individual to whom the *information* relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the *information*:

i. is accurate; and

ii. having regard to the purpose for which the *information* was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading.

b. if UOW is not prepared to amend *information* in accordance with a request by the individual to whom the *information* relates, UOW must, if requested by the individual concerned, take such steps as are reasonable to attach to the *information* any statement provided by that individual of the amendment sought, in such a manner that it is capable of being read with the *information*,

c. if *information* is amended in accordance with this principle, the individual to whom the *information* relates is entitled, if it is reasonably practicable, to have recipients of that *information* notified of the amendments made by UOW.

Exceptions

2. Exceptions to IPP 8 and HPP 8 include where:

a. UOW is lawfully authorised or required not to comply; or

b. non-compliance is otherwise permitted (or necessarily implied or reasonably

contemplated) under an Act or any other law.

Application by UOW

3. UOW holds *information* in a variety of systems for UOW purposes.
4. UOW may amend *information* it holds which an individual believes to be incorrect or inappropriate.
5. If UOW elects not to amend that *information* held, UOW will, where practicable, (depending on the capabilities of the system used) attach a note to that *information* of the amendment or addendum sought.
6. Where *information* held by UOW is amended, UOW will notify the recipients of that *information* of the amendment, so far as it is reasonably practical. The following factors will be taken into account on a case by case basis when determining whether it is reasonably practical to notify others of the amendment:
    a. who the recipients of the *information* are;
    b. the purpose for which the *information* was collected;
    c. the sensitivity of the *information*;
    d. the importance of the accuracy of the *information*;
    e. the potential effects on the individual concerned if the *information* is inaccurate, out of date or irrelevant;
    f. any future opportunities to correct inaccuracies before the *information* is used; and
    g. the ease and associated costs of notifying recipients.

12 UOW must check accuracy of *information* before use

1. IPP 9 and HPP 9 state that if UOW holds *information*, it must not use that *information* without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the *information* is proposed to be used, the *information* is relevant, accurate, up to date, complete and not misleading.

Application by UOW

2. UOW will take one or more of the following factors into account to determine whether the *information* it holds is relevant, accurate, up to date, complete and not misleading:
    a. the purpose for which the *information* was collected;
    b. the sensitivity of the *information*;
    c. how many people have access to the *information*;
    d. the importance of accuracy to the proposed use;
    e. the potential effects on the individual concerned if the *information* is inaccurate, out-of-date or irrelevant;
    f. the opportunities to subsequently correct the *information*; and
    g. the ease with which the *information* can be checked.

3. Examples where UOW checks the accuracy of *information* before use include:

   a. checking student enrolment information such as visa and immigration, pre-requisites, academic results and so on;
   b. checking employee references, work history, academic qualifications and identification, as well as the employee rights to work in Australia; and
   c. checking *information* provided in higher degree research (HDR) applications.

13 Limits on Use and Disclosure of *Personal Information*

1. In general terms, 'use' refers to the communication or handling of *information* within UOW, whereas 'disclosure' refers to the communication or transfer of *information* outside UOW, other than to the individual concerned. The rules relating to use and disclosure of *personal information* are discussed below.

2. Use of *personal information*:

IPP 10 states that UOW must not use personal information it holds for a purpose other than that for which it was collected unless:

   a. the individual to whom the *personal information* relates has consented to the use of the *personal information* for that other purpose, or

   b. the other purpose for which the *information* is used is directly related to the purpose for which the *personal information* was collected, or

   c. the use of the *personal information* for that other purpose is necessary to lessen or prevent a serious and imminent threat to the life or health of any individual.

2. Disclosure of *personal information*:

IPP 11 states that UOW must not disclose *personal information* it holds without consent (other than to the individual to whom the *personal information* relates) unless:

   a. the individual concerned is reasonably likely to have been aware, or has been made aware at collection, that *personal information* of that kind is usually disclosed to that other person or body; or

   b. the disclosure is directly related to the purpose for which the *personal information* was collected and UOW has no reason to believe that the individual concerned would object to the disclosure; or

   c. the disclosure of the *personal information* is necessary, on reasonable grounds, to prevent or lessen a serious and imminent threat to the life or health of any individual.

2. Special restrictions on disclosure of personal information:

IPP 12 states that, in addition to the principles of IPP11, UOW must not disclose *personal information* to any person or body who is in a jurisdiction outside NSW or to a Commonwealth agency unless:

   a. UOW reasonably believes that the recipient of the *information* is subject to a law, binding scheme or contract that upholds the principles for the fair handling of *personal information* that are substantially similar to the principles of NSW privacy laws; or

   b. the individual expressly consents to the disclosure; or

c. the disclosure is necessary for the performance of a contract between the individual and UOW; or

d. the disclosure is necessary, on reasonable grounds, to prevent or lessen a serious and imminent threat to the life or health of any individual; or

e. the disclosure is permitted or required by an Act (including an Act of the Commonwealth) or any other law; or

f. UOW has taken reasonable steps to ensure that the *personal information* disclosed will be handled in a manner that is consistent with NSW privacy laws.

2. Disclosure of *sensitive information*:

IPP12 states that UOW must not disclose sensitive information unless the disclosure is necessary to prevent a serious and imminent threat to the life or health of the individual concerned, or another person.

Exceptions

2. Exceptions to IPP 10 include where:

a. it is reasonably necessary to exchange *personal information* within UOW for law enforcement purposes or for the protection of the public revenue; or

b. the use of the *personal information* is reasonably necessary to enable UOW to investigate or handle a complaint or other matter that could be referred or made to an *investigative agency*, or that has been referred or made from an *investigative agency*.

3. Exceptions to IPP 11 include where the disclosure of the *personal information* concerned is:

a. made in connection with proceedings for an offence; or

b. for law enforcement purposes; or

c. reasonably necessary for the protection of public revenue; or

d. reasonably necessary in order to investigate an offence where there are reasonable grounds to believe that an offence may have been committed; or

e. authorised or required by subpoena, search warrant or other legal order; or

f. made to a *law enforcement agency* for the purpose of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person; or

g. made to an *investigative agency* as a result of an investigation from a complaint or other matter that was either made or referred from an *investigative agency* or that could have been referred or made by UOW to the *investigative agency*.

4. Exceptions to IPP 12 exist, including where:

a. the disclosure is reasonably necessary for the purposes of law enforcement in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed;

b. the use and/or disclosure:

i. is lawfully authorised or required not to comply with this IPP; or

ii. non-compliance is otherwise permitted (or necessarily implied or reasonably contemplated) under an Act or any other law; or

iii. has been expressly consented to by the individual about whom the *sensitive information* relates; or

iv. the disclosure is made from UOW to another public sector agency under the administration of the same Minister or the Premier in certain circumstances.

5. UOW is not required to comply with IPP 10 and/or IPP 11 if:

   a. it is lawfully authorised or required not to comply with IPP 10 and/or IPP 11; or

   b. non-compliance is otherwise permitted (or necessarily implied or reasonably contemplated) under an Act or any other law (this includes the State Records Act); or

   c. the individual to whom the *personal information* relates, has expressly consented to the use and/or disclosure; or

   d. the disclosure is made from UOW to another public sector agency under the administration of the same Minister or Premier in certain circumstances; or

   e. the use or disclosure is reasonably necessary for the purpose of research, or the compilation or analysis of statistics, in the public interest, and:

      i. either the purpose cannot be served by de-identified *personal information* and it is impracticable to seek the consent of the individual for the use/disclosure, or reasonable steps are taken to de-identify the *personal information*; and

      ii. if it could reasonably be expected to identify individuals, the *personal information* is not published in a generally available publication; and

      iii. the use of the *personal information* is in accordance with the statutory guidelines issued under PPIPA by the Privacy Commissioner; or

   f. it is reasonably necessary for the *personal information* to be exchanged with another public sector agency to enable inquiries to be referred between the agencies concerned or to enable the auditing of accounts or the performance of an agency.

Application by UOW

2. UOW obtains specific consent for certain uses and disclosure when collecting *personal information*. As an example, during the enrolment process students provide consent to UOW using and/or disclosing that student's *personal information* for stated primary purposes and secondary purposes reasonably related to those primary purposes. This puts students on notice about the use and disclosure of their *personal information* by UOW and its *related entities.*

3. Other examples relating to informed use and disclosure include where UOW verify and exchange *personal information* with:

   a. other educational institutions for cross-institutional study purposes and/or verification of academic transcripts or transfers; or

   b. external bodies for the purpose of verification of qualifications, accreditation, professional qualifications or membership with that external body; or

c. previous employers of prospective *staff*.

4. UOW applies learning analytics initiatives to the student data it holds in order to maximise each student's academic success and support their student learning experience. This is achieved by giving each student and their teachers access to the student's learning-related information in order to build on that student's areas of strength, identify areas for improvement and to utilise support services offered by UOW.

5. The Student Privacy and Disclosure Statement provides details of the various ways in which UOW may use and disclose *personal information* collected from students This consent statement may be amended if necessary and the student will be notified of the updated consent statement when any variation to enrolment is made by the student.

6. The Privacy Collection Statement for Recruitment and Employee Records provides details of the various ways in which UOW may use and disclose *personal information* collected from current or prospective employees. Employees acknowledge their understanding of this statement as part of their Acceptance of Offer for employment.

7. Examples where UOW uses *personal information* for a purpose that is directly related to the primary purposes for which it was collected include:

    a. compilation of UOW reunion and event invitation lists;

    b. preparation of testimonials;

    c. preparation of graduate destination surveys;

    d. commercial relationships;

    e. UOW news and updates;

    f. fundraising;

    g. promotion of events and programs (including postgraduate study programs);

    h. surveys and competitions;

    i. engagement in research; or

    j. prospective research.

8. Where *personal information* is used for direct marketing purposes, UOW will make all efforts to apply the principles of the Commonwealth Privacy Act as best practice. This includes providing a clear mechanism through which an individual may choose to unsubscribe from receiving any further messages from UOW.

9. UOW is required by law to disclose certain information to various Government agencies. For example:

    a. as part of its mandatory reporting process, UOW must disclose *personal information* to various Government agencies. Examples are the Commonwealth government department with responsibility for immigration, the Commonwealth government department with responsibility for tertiary education and the Australian Taxation Office (ATO);

    b. under the *Public Interest Disclosures Act 1994* (NSW) or its equivalent, UOW may be obliged to make a disclosure regarding corruption, maladministration or other conduct

governed by that Act;

c. as part of its mandatory notification obligations, UOW must disclose *personal information* to certain *investigative agencies* such as the Australian Health Practitioners Regulation Agency.

10. Where UOW receives a request from a Commonwealth government agency to provide *personal information*, UOW will:

    a. only disclose the *personal information* that UOW is authorised to disclose under relevant legislation;

    b. only provide the *personal information* that falls within the scope of the request;

    c. keep a written record of the *personal information* that has been disclosed.

UOW has developed an Information Sheet – Centrelink (Human Services) Inquiries to assist staff to respond to requests for information from Human Services.

2. Where *personal information* is to be disclosed to a *law enforcement agency*, UOW will:

    a. only provide the *personal information* that is relevant and necessary for the intended purpose;

    b. obtain and document proof that the individual seeking the *personal information* is a representative of the appropriate *law enforcement agency*; and

    c. keep a written record of the *personal information* that has been disclosed.

UOW has developed an Information Sheet – Requests for Information from Police to assist *staff* to respond to requests for *information* from police.

2. UOW may receive requests from *law enforcement agencies* for disclosure of *sensitive information*. In such circumstances, and considering the special restrictions applied to such *sensitive information*, UOW's Privacy Officer may refuse to comply in the absence of a subpoena or warrant or similar legal order, or require the *law enforcement agency* to satisfy UOW that the release of such *sensitive information* will not breach PPIPA.

3. Where *personal information* or *sensitive information* is to be disclosed under a subpoena or warrant or similar legal order, UOW will:

    a. only provide the information that is within the scope of the order; and

    b. keep a written record of the information that has been disclosed.

UOW has developed an Information Sheet – Records Requested under Subpoena to assist *staff* to respond to requests for *information* under a subpoena.

2. If UOW is part of an investigation by an *investigative agency*, UOW's cooperation may be mandatory, including providing access to *personal information* that is beyond the purposes for which that *information* was collected.

3. UOW welcomes enquiries and feedback (which includes comments, compliments and complaints) from *staff*, students and third parties. *Personal information* may be used to respond to any matters raised through these communication systems to improve UOW services and promote effective complaint handling processes.

4. Where UOW engages the services of a third party for the purpose of providing a particular

service to UOW, all reasonable steps will be taken to ensure that the third party has robust practices in place to protect the *information* and prevent its unauthorised use or disclosure. The third parties to whom we disclose personal information may be located in Australia and other countries. Section 23 of this Privacy Management Plan provides further information on Third Party Engagement and Confidentiality.

14 Limits on Use and Disclosure of *Health Information*

1. In general terms, 'use' refers to the communication or handling of *information* within UOW, whereas 'disclosure' refers to the communication or transfer of *information* outside UOW, other than to the individual concerned. The rules relating to use and disclosure of *health information* are discussed below.
2. HPP 10 and HPP 11 state that UOW must not use or disclose *health information* for another purpose (secondary purpose) other than the primary purpose for which it was collected unless:
    a. the individual has provided consent;
    b. the secondary purpose is directly related to the primary purpose and within the expectations of the individual;
    c. it is reasonably believed to be necessary to lessen or prevent;
        i. a serious and imminent threat to the life or health of the individual concerned or another person; or
        ii. a serious threat to public health or public safety.

Exceptions

2. Exceptions to HPP 10 and HPP 11 include where the use and/or disclosure is:
    a. made to a law enforcement agency for law enforcement and related matters such as:
        i. for the purposes of ascertaining the whereabouts of an individual who has been reported to police as a missing person, or
        ii. where there are reasonable grounds to believe that an offence may have been, or may be, committed; or
    b. lawfully authorised or required, or permitted under another law to do so, such as subpoena or search warrant; or
    c. reasonably necessary to enable UOW to investigate or handle a complaint or other matter that may be referred or made to an investigative agency, or that has been referred or made from an investigative agency; or
    d. necessary to be used by UOW as a part of its investigation, or in the reporting of its concerns to relevant persons or authorities, where UOW has reasonable grounds to suspect that:
        i. unlawful activity has been or may be engaged in, or
        ii. person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under the Health Practitioner Regulation National Law (NSW), or

iii. a UOW employee has or may have engaged in conduct that may be grounds for disciplinary action such as a breach of UOW's Code of Conduct; or

e. reasonably necessary for the funding, management, planning or evaluation of health services, or for the training of UOW employees or persons working with UOW, or for research, or the compilation or analysis of statistics, in the public interest and;

i. either the purpose cannot be served by de-identified health information and it is impracticable to seek the consent of the individual for the use/disclosure, or reasonable steps are taken to de-identify the health information; and

ii. if it could reasonably be expected to identify individuals, the health information is not published in a generally available publication; and

iii. the use of the health information is in accordance with the statutory guidelines issued under HRIPA by the Privacy Commissioner; or

f. made to an immediate family member for compassionate reasons, and

i. the disclosure is limited to the extent reasonable for those compassionate reasons; and

ii. the individual is incapable of giving consent; and

iii. the disclosure is not contrary to any wish expressed by the individual (and not withdrawn) of which UOW was aware or could make itself aware by taking reasonable steps; and

iv. if the immediate family member is under the age of 18 years, UOW reasonably believes that the family member has sufficient maturity in the circumstances to receive the health information; or

v. made from UOW to another public sector agency under the administration of the same Minister or Premier in certain circumstances.

3. UOW is not required to comply with HPP 10 and/or HPP 11 if:

a. it is lawfully authorised or required not to comply with HPP 10 and/or HPP 11; or

b. non-compliance is otherwise permitted (or necessarily implied or reasonably contemplated) under an Act or any other law (this includes the State Records Act); or

c. the disclosure is made from UOW to another public sector agency under the administration of the same Minister or Premier in certain circumstances.

Application by UOW

4. UOW obtains specific consent for certain uses and disclosure when collecting *health information*. As an example, during the enrolment process students provide consent to UOW using and/or disclosing that student's *health information* for stated primary purposes and secondary purposes reasonably related to those primary purposes. This puts students on notice about the use and disclosure of their *health information* by UOW and its *related entities*.

5. The Student Privacy and Disclosure Statement provides details of the various ways in which UOW may use and disclose *health information* collected from students. Any updates to this

consent statement will be provided to the student when any variation to enrolment is made by the student.

6. The Privacy Collection Statement for Recruitment and Employee Records provides details of the various ways in which UOW may use and disclose *health information* collected from current or prospective employees. Employees acknowledge their understanding of this statement as part of their Acceptance of Offer for employment.

7. UOW may be required to disclose *health information* under laws, including:

   a. under search warrants, subpoenas, other legal orders or statutory instruments;

   b. reporting of notifiable diseases pursuant to, for example, the *Public Health Act 2010*. Examples of notifiable diseases include, but are not limited to, Hepatitis A, B, C, D, E, Diphtheria, Tetanus, Pertussis and Tuberculosis.

8. Where UOW intends to use and/or discloses *health information* for the purposes of providing training or relating to research, and it is impracticable to seek consent, it will take all reasonable steps to de-identify the *health information*. If the *health information* could reasonably be expected to identify individuals, UOW will ensure that *health information* is not published in a generally available publication or in a form that identifies individuals.

9. Where research relating to humans is to be undertaken, UOW has established a Human Research Ethics Committee to approve the research proposal before use or disclosure of *health information* occurs.

10. UOW may also verify and exchange *health information* with an external placement body for the purpose of clinical or other placement or practicum experience which is required by a course of study at UOW or is otherwise approved by UOW. This may include notifying the student placement provider of *health information* relevant to the student placement, in consultation with the student. Examples include pre-existing medical conditions that could affect a student's placement activities and/or UOW's student personal accident insurance cover.

11. UOW also has various reporting requirements under Commonwealth and State Government legislation and *health information* may lawfully be used and/or disclosed for those purposes.

12. Where *health information* is to be disclosed to a *law enforcement agency*, UOW will:

    a. only provide the *health information* that is relevant and necessary for the intended purpose;

    b. obtain and document proof that the person seeking the *health information* is a representative of the appropriate *law enforcement agency*;

    c. keep a written record of the *health information* that has been disclosed.

UOW has developed an Information Sheet – Requests for Information from Police to assist *staff* to respond to requests for *information* from police.

2. Where *health information* is to be disclosed under a subpoena, warrant or similar legal order, UOW will:

   a. only provide the *health information* that is within the scope of the legal order; and

   b. keep a written record of the *health information* that has been disclosed.

UOW has developed an Information Sheet – Records Requested under Subpoena to assist *staff* to respond to requests for *information* under a subpoena.

2. UOW may need to use *health information* for the purpose of providing relevant student services. For example, a student may register with Disability Services as someone suffering a disability, and it may be important for other areas of UOW to be aware of the student's condition. For example, Disability Services may provide that *health information* to the Student Services Division for arrangement of appropriate examination supervision.

3. UOW welcomes enquiries and feedback (which includes comments, compliments and complaints) from staff, students and third parties. *Health information* may be used to respond to any matters raised through these communication systems to improve UOW services and promote effective complaint handling processes.

15 Other Health Privacy Principles

1. **HPP 12 – Identifiers**

UOW may only assign identifiers (eg, a number) to individuals, and use and disclose those identifiers, if necessary to enable UOW to carry out any of its functions efficiently.

2. **HPP 13 – Anonymity**

Wherever it is lawful and practicable, UOW will give individuals the opportunity to not identify themselves when entering into transactions with or receiving health services from UOW.

2. **HPP 14 – Transborder data flows and data flow to Commonwealth agencies**

UOW will not transfer health information about an individual to an organisation located outside New South Wales or to a Commonwealth agency unless:

a. the recipient is subject to principles that are substantially similar to the NSW HPPs; or

b. the individual consents to the transfer; or

c. the transfer is necessary for the performance of a contract between the individual and UOW; or

d. the transfer is necessary for the performance of a contract in the interest of the individual between UOW and a third party; or

e. the transfer is for the benefit of the individual and it is impracticable to obtain the consent of the individual to that transfer and the individual would otherwise be likely to give consent; or

f. the transfer is necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual or another person or a serious threat to public health or public safety; or

g. UOW has taken reasonable steps to ensure that the transferred health information will not be held, used or disclosed by the recipient inconsistently with the NSW HPPs; or

h. the transfer is otherwise permitted or required by law.

2. **HPP 15 – Linkage to Health Records**

UOW will not include health information about an individual or an identifier (eg, a number) of an

individual in a state or national health records linkage system without the individual 's express consent.

Exceptions

2. Exceptions to HPP 15 apply, including that non-compliance is permitted by law or the use and disclosure otherwise complies with HPP 10 and HPP 11.

16 Application of Commonwealth Privacy Act

1. UOW is a statutory corporation established under the *University of Wollongong Act 1989* (NSW), and as such, is not an agency that falls within the scope of the Commonwealth Privacy Act.
2. Any collection of *personal information* that is expressly governed by the Commonwealth Privacy Act will be managed in accordance with the requirements of that Act. An example is where UOW collects tax file numbers from employees.
3. UOW's *related entities* are corporations established under the *Corporations Act 2001* (Cth) and as such are required to comply with both Commonwealth and NSW privacy legislation. For more information on a specific *related entity's* privacy compliance, please contact that *related entity*.

17 Public Registers Held by UOW

1. PPIPA requires agencies with responsibilities for public registers to comply with certain requirements.
2. A public register is defined in PPIPA and HRIPA as:

"A register of personal or health information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee)"

2. UOW has the following public registers:
   a. A contracts register as part of its *Government Information Public Access Act 2009* (NSW) mandatory disclosure obligations, available on UOW's website; and
   b. A register of the names of UOW graduates known as the graduate roll, available on UOW's website.
3. An individual who does not wish to have his/her *personal information* accessible on a UOW public register should contact Student Central on 1300 275 869 or email askuow@uow.edu.au . UOW will manage such requests on a case by case basis.

18 Offences

1. It is an offence under PPIPA and HRIPA for UOW staff, as part of his/her employment, to:
   a. intentionally disclose or use *information* that the staff member has accessed, unless it is for a lawful or authorised purpose; and/or
   b. supply, by way of a bribe or other similar corrupt conduct, any *information* about an individual to another individual.

UNIVERSITY OF WOLLONGONG AUSTRALIA

19 Complaints and/or Internal Reviews

1. An individual who has a grievance about the way in which UOW has managed his/her *information* is entitled to a review of UOW's conduct ("Internal Review")
2. A request for Internal Review can only be made where it is alleged that UOW's conduct has:
   a. breached any of the Information Protection Principles in PPIPA or any of the Health Privacy Principles in HRIPA; or
   b. breached a privacy code of practice that applies to UOW; or
   c. disclosed *personal information* kept in a public register.
3. UOW encourages individuals who have privacy complaints to contact one of UOWs Privacy Officers so that, where possible, issues may be easily and speedily resolved through existing policies and complaint handling procedures. Where an individual remains dissatisfied or concerned following the outcome as a result of UOW's complaint handling procedures, the individual may wish to proceed with an Internal Review, if applicable. An individual may also contact the Information and Privacy Commission NSW to discuss any concerns relating to privacy. Where a concern relates to UOW's conduct referred to in 2a-2c above, the Privacy Commissioner may recommend that it would be more appropriate for an internal review application to be made.
4. Information on how to contact a UOW Privacy Officer can be found in the Roles and Responsibilities section of this Plan or on UOW's privacy homepage at http://www.uow.edu.au/about/privacy/index.html.

How to Make an Internal Review Application

2. An application for an Internal Review of UOW's conduct should:
   a. be in writing;
   b. be addressed to UOW;
   c. specify a return address in Australia; and
   d. be lodged with a UOW Privacy Officer within 6 months of the date the applicant first became aware of the alleged conduct. UOW may exercise its discretion to accept an application which may be received after the end of the 6 month period.
3. A Privacy Complaint Internal Review Application Form which is available on UOW's privacy homepage should be completed and submitted to UOW.

Who Will Conduct the Internal Review

2. The Internal Review will be conducted by a UOW Privacy Officer without any conflict of interest and/or involvement in the conduct which is the subject of the application. In the case of any conflict of interest, a senior staff member with no conflict of interest will conduct the Internal Review, depending on the circumstances.

How Will the Internal Review be Conduct

2. Internal Reviews will be conducted in accordance with the requirements of Part 5 of PPIPA and with regard to any guidance produced by the NSW Privacy Commissioner.

3. On receiving an application for an Internal Review UOW must, as soon as practicable, inform the Information and Privacy Commission NSW of the complaint and provide that office with a copy of the Internal Review application. The Privacy Commissioner must be kept informed of the outcome of the Internal Review and any action UOW proposes to take as a result of the Internal Review.
4. The Privacy Officer dealing with the Internal Review (the reviewing officer) will assess the application and inform the applicant in writing of the following:
    a. the name, title and contact details of the reviewing officer;
    b. the reviewing officer's understanding of the conduct complained about and the privacy principle/s at issue;
    c. that UOW is conducting the review under PPIPA or HRIPA, as appropriate;
    d. how the reviewing officer is independent of the person/s responsible for the alleged conduct;
    e. the required completion date for the review process (maximum of 60 days);
    f. that an external review may be lodged with the NSW Civil and Administrative Tribunal (NCAT) if the review is not completed within the required timeframe; and
    g. that the Information and Privacy Commission NSW will be kept informed of the progress and findings of the Internal Review.
5. UOW must consider any relevant material submitted by the applicant or by the Information and Privacy Commission NSW during the Internal Review.
6. UOW will complete the Internal Review within 60 days of receipt of the Internal Review application, failing which the applicant has a right to seek a review of UOWs conduct complained about by the NSW Civil and Administrative Tribunal.
7. The reviewing officer will follow the steps as set out in the 'Internal Review Checklist for the Respondent Agency' published by the Information and Privacy Commission NSW.
8. Once the Internal Review has been completed, UOW may do one or more of the following:
    a. take no further action on the matter;
    b. make a formal apology to the applicant;
    c. take such remedial action as it thinks appropriate;
    d. provide undertakings that the conduct will not occur again; and/or
    e. implement administrative measures to ensure that the conduct will not occur again.
9. Within 14 days of the completion of the Internal Review, UOW will notify the applicant in writing of:
    a. the findings of the Internal Review (and the reasons for those findings);
    b. the action proposed to be taken by UOW (and the reasons for taking them); and
    c. the right of the individual to have those findings, and the proposed action, reviewed by the NSW Civil and Administrative Tribunal.

Appeals

2. An applicant who has lodged an Internal Review application is entitled to seek a review by the NSW Civil and Administrative Tribunal of the conduct complained about if:
   a. the applicant is not satisfied with the findings of the Internal Review; or
   b. the applicant is not satisfied with the proposed actions to be taken by UOW; or
   c. UOW has not dealt with the Internal Review application within the required 60 day timeframe.

Reporting

2. UOW is obliged to provide statistical details on privacy activities in its annual report to NSW Parliament, including statistics about Internal Review applications.

20 Training and Education

1. UOW has a training and implementation program regarding privacy, including:
   a. providing privacy training as part of *staff* induction;
   b. notifying new *staff* of their privacy obligations within their employment documents;
   c. maintaining a privacy homepage which contains a range of information about privacy, including a Privacy Awareness e-book and FAQ section;
   d. providing information sheets to assist *staff* when dealing with requests from police or from Commonwealth government agencies such as Centrelink, or in response to subpoenas or summons;
   e. implementing and maintaining:
      i. UOW's Privacy Policy;
      ii. this Privacy Management Plan; and
      iii. UOW's Privacy Information Sheet.
   f. providing privacy education via newsletters, information sessions, workshops and online training modules;
   g. providing privacy advice on a case by case basis to *staff*; and
   h. UOW Privacy Officers participating in the NSW privacy practitioners' group meetings held quarterly.

21 Policies that Ensure Compliance with Privacy Legislation

1. UOW's policies on managing *information* reflect the requirements of applicable legislation, NSW government policy, guidelines and appropriate Australian Standards.
2. The following list provides examples of policies and procedures adopted by UOW that assist it to comply with its privacy obligations:
   a. Privacy Policy;
   b. The University Code of Conduct;

c. Records Management Policy;

d. Information Technology policies such as IT Acceptable Use Policy;

e. Fraud and Corruption Prevention Policy;

f. Code of Practice – Student Professional Experience;

g. Critical Incident Guidelines;

h. CCTV Surveillance Standard; and

i. Student Health Assessment and Leave Policy.

22 Legislation Affecting UOW's Management of *Information*

1. The following list provides examples of legislation that affects particular aspects of *information* management by UOW:

   a. Workplace Surveillance Act 2005 (NSW);

   b. Independent Commission Against Corruption Act 1988 (NSW);

   c. Government Information (Public Access) Act 2009 (NSW);

   d. State Records Act 1998 (NSW);

   e. Public Interest Disclosures Act 1994 (NSW);

   f. Medical Board of Australia Health Practitioner Regulation National Law 2009 (NSW);

   g. Anti-Discrimination Act 1977 (NSW);

   h. Disability Discrimination Act 1992 (Cth).

   i. Higher Education Support Act 2003

23 Third Party Engagement and Confidentiality

1. Where UOW is required to share particular *information* with a contractor, agent or consultant engaged to undertake work for/with UOW (third party), UOW will take reasonable steps to ensure that the service provider has adequate measures in place to protect the *information* and does not inappropriately use or disclose the *information*. The third parties to whom UOW may disclose *information* may be located in Australia and other countries.

2. UOW will take all reasonable steps to include provisions in its contracts with those third parties that:

   a. the third party is to comply with PPIPA and/or HRIPA or principles that are substantially similar to PPIPA and/or HRIPA;

   b. the third party must treat all data (whether provided by UOW, uploaded by users or generated by any applicable software) in a confidential manner and only use *information* for the sole purpose for which it was provided to the third party;

   c. the third party must minimise opportunities for misuse of the *information,* such as restricting access to the *information* by its employees and/or contractors; and

d. control the disposal and/or return of the *information* to UOW once the service is completed.

3. Each *staff* member is expected to maintain the confidentiality of confidential information that *staff* members access in the course of their employment. This obligation of confidentiality includes the appropriate management of and compliance with UOW 's Privacy Policy and this Privacy Management Plan when dealing with *information*.

4. From time to time, UOW may require a *staff* member to enter into a non-disclosure agreement about certain categories of *information* held by UOW.

24 Roles & Responsibilities

1. UOW's Privacy Officers are:

   a. Manager, Information Compliance, Legal Services Unit – as Privacy Officer and main contact person for privacy issues – phone 02 4221 4368 or email privacy-enquiry@uow.edu.au;

   b. Director, Governance and Legal Division as Principal Privacy Officer;

   c. Senior Manager, Senior Lawyer and Lawyers, Legal Services Unit as Privacy Officers.

2. The Privacy Officers are responsible for:

   a. training and education of *staff* on privacy;

   b. providing advice to *staff* on privacy issues;

   c. liaising with privacy agencies such as the Information and Privacy Commission NSW;

   d. responding to privacy complaints and conducting internal reviews;

   e. implementing and maintaining UOW's Privacy Policy and this Privacy Management Plan;

   f. ensuring UOW's privacy homepage at http://www.uow.edu.au/about/privacy/index.html contains current, relevant privacy information; and

   g. preparing mandatory reports relating to privacy.

3. All *staff* are responsible for complying with UOW's privacy obligations when handling *information*;

4. The Human Resources Division is responsible for the central management of *staff information*;

5. The Student Services Division is responsible for the central management of student *information*;

6. The Graduate Research School is responsible for the central management of higher degree research (HDR) student *information*;

7. For further information in relation to this Privacy Management Plan, please contact:

   Manager, Information Compliance

   Administration Building (36)

UNIVERSITY OF WOLLONGONG NSW 2522

Phone: 4221 4368

Email: privacy-enquiry@uow.edu.au

UNIVERSITY OF WOLLONGONG AUSTRALIA

25 Version Control Table

Version Control	Date Effective	Approved By	Amendment
1	7 December 2012	University Council	New Privacy Management Plan
2	16 December 2016	Vice-Chancellor	Amendments including name change to UOW's related entity, UOW divisions and various government departments. Addition of various statements demonstrating UOW's application of the privacy principles and amendments to reflect change in legislation.
3	15 February 2019	University Council	Consequential amendments as a result of the rescission of the Access to Information Policy.